State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

April 12, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-058

DATE(S) ISSUED:
04/12/2016

SUBJECT:
Cumulative Security Update for Internet Explorer (MS16-037)

OVERVIEW:
Multiple vulnerabilities have been discovered in Internet Explorer that could allow for remote code execution. These vulnerabilities could allow an attacker to execute code in the context of a user who views a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild. CVE-2016-0160 has been publicly disclosed.

SYSTEMS AFFECTED:

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities exist in Internet Explorer. The vulnerabilities are as follows:

- Four Memory Corruption Vulnerabilities exist that could execute code in the context of the current user (CVE-2016-0154, CVE-2016-0159, CVE-2016-0164, CVE-2016-0166).
- One DLL Remote Code Execution Vulnerability exists when Internet Explorer improperly validates input before loading dynamic link library (DLL) files (CVE-2016-0160).
- One Information Disclosure Vulnerability when Internet Explorer does not properly handle Javascript(CVE-2016-0162).

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS16-037

CVE:

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0154
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0159
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0160
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0162
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0164
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0166